

$$T_N = f_N(T)$$

$$T'_N = T_N \pmod{H_j^i}$$

$$k = H_j^i(T'_N)$$

$$i \in S_j^i$$

$$T' = f_R(T)$$

Figure 1

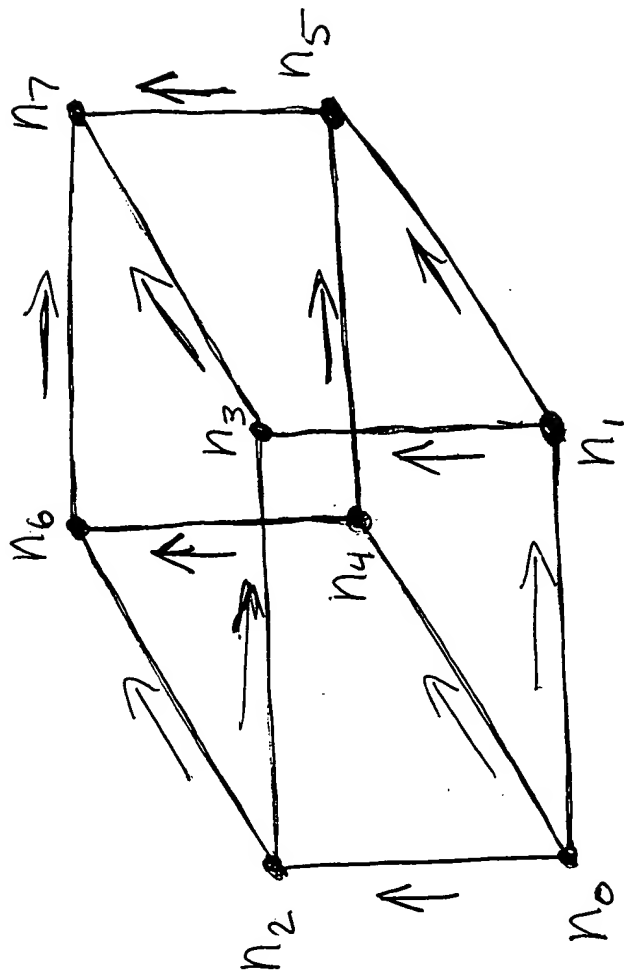


Figure 2